ALPHA SHIELD®

INTERNET PRIVACY PROTECTION

[For Broadband cable, DSL, ISDN, Wireless]

MANUAL DEL USUARIO


internet

Índice

Revisión 1.4

Introducción

AlphaShield ™

Enhorabuena por la compra del nuevo dispositivo de seguridad AlphaShield™. La adquisición del producto AlphaShield™ le proporciona total tranquilidad al conectarse a Internet mediante conexiones continuas con módem cable o xDSL. El AlphaShield ™ es un dispositivo "plug and play" (enchufar y listo) que no requiere software ni configuración de ningún tipo. Proporciona al usuario final un algo grado de seguridad en las conexiones de red y PC.

El AlphaShield™ es un dispositivo seguro que proporcionará años de operación sin problemas. No son necesarios parches, controladores de software actualizados ni ningún mantenimiento. El AlphaShield™ puede conectarse y estar funcionando en tan solo unos minutos y no requiere ninguna formación ni herramientas especiales. Una vez instalado, el usuario no tiene que apagar o desconectar el ordenador de la red para obtener seguridad.

El AlphaShield™ utiliza una tecnología Gap pendiente de patente denominada **AlphaGap™**. Esta tecnología se utiliza para proporcionar al usuario el mayor nivel de seguridad de red. Además, el AlphaShield™ incorpora las tecnologías **RPA** (Real-Time Packet Authorization) e **IP Stealth**, las cuales gestionan conexiones de usuarios seguras a la red o a Internet.

La combinación de estas tres tecnologías ha demostrado que el AlphaShield™ es un dispositivo de seguridad de red totalmente fiable. Esta solución de seguridad no actúa como las pasarelas (gateways) o firewalls (cortafuegos) convencionales que poseen una dirección IP asociada. El AlphaShield™ no posee ninguna asignación de dirección IP y además, oculta la dirección IP del ordenador conectado. Posee su código operativo de propiedad almacenado en una memoria no volátil inaccesible e inalterable desde los puertos de conexión del usuario o de la red.

Características y beneficios

El AlphaShield™ es la siguiente generación en seguridad de red. Es un dispositivo de hardware externo autónomo que utiliza tecnología punta para detener a los hackers y los ataques de red antes de que puedan acceder al ordenador. AlphaShield ™ supervisa todas las transmisiones de datos de entrada y de salida entre su ordenador y el mundo exterior. Realiza todo este proceso de forma continua, manteniendo la conexión a Internet. AlphaShield™ posee muchas características avanzadas que le convierten en un dispositivo de seguridad sólido, por ejemplo:

· Tecnología "GAP" exclusiva (Marca registrada AlphaGap™)

· RPA (Real-Time Pachet Authorization, propiedad de AlphaShield™)

· Tecnología IP Stealth (Oculta la asignación de la dirección IP cliente)

· Centinela de hardware autónomo

· **Modo Manual** (conexión temporizada con una desconexión lógica)

· **Modo Automático** (conexión continua, desconexión lógica opcional)

· **Modo Bloqueo** (conexión temporizada con una desconexión física)

· Función de conexión/desconexión manual instantánea

· Puerto auxiliar para otros dispositivos IP

El AlphaShield™ proporciona muchos beneficios que lo convierten en un líder en seguridad de datos y privacidad en Internet, como por ejemplo:

- Se conecta y desconecta sin interrumpir el servicio de Internet
- Verdadera instalación y operación "plug and play"
- Arquitectura de baja latencia (funciona a velocidad de cable)
- No es necesario poseer conocimientos técnicos para la configuración y la instalación
- No son necesarios ningún parche de software ni actualización
- Funciona con todas las plataformas de sistema operativo
- No se requiere ningún software en el sistema del cliente
- Compatible con Cable, xDSL, ISDN o banda ancha sin cable
- Firmware inmune a virus y alteraciones
- No utiliza ningún recurso del sistema (CPU autónoma)
- No es incompatible con los firewalls (cortafuegos) o direccionadores (routers) existentes
- Elimina los ataques DOS (Ataques de denegación de servicio)
- Proporciona protección en línea 24 horas 7 días a la semana

Instalación y operación

Para instalar el nuevo AlphaShield™ en el PC de su casa, realice los pasos siguientes. Si al realizar alguno de los pasos no obtiene el resultado previsto, consulte la guía de resolución de problemas de este manual.

(1) Extraiga el AlphaShield™ de la caja y asegúrese de que contiene los siguientes elementos

Un dispositivo de seguridad AlphaShield™.
Un adaptador de alimentación Universal de 9 voltios CC, 300 mA.
Un cable de red directo RJ-45 de 2m aprox.
Una guía de Instalación y de Usuario.

(2) Enchufe el AlphaShield™ con el adaptador CA universal.

Introduzca el enchufe redondo del adaptador de alimentación en el enchufe hembra de alimentación del AlphaShield™.
Enchufe el adaptador CC universal de 9 voltios en un enchufe de pared estándar.
Asegúrese de que el LED central de Conexión del AlphaShield™, situado en la parte frontal, se ilumina de color rojo.

(3) Conecte el AlphaShield™ al módem externo Cable o xDSL.

Utilice un cable RJ-45 directo para conectar el módem cable o xDSL a la entrada RJ-45 del AlphaShield™.

Si lo ha conectado correctamente, el indicador LED de Datos de salida se iluminará de color verde.

(4) Conecte el AlphaShield™ al PC.

Utilice el cable RJ-45 directo de casi 2 metros para realizar la conexión Ethernet del ordenador al RJ-45 PC Ethernet del AlphaShield™. Si lo ha conectado correctamente, el indicador LED de datos de salida se iluminará en verde.

(5) Seleccione el modo de seguridad en el que desea que AlphaShield™ funcione.

Utilice el interruptor de modo situado en la parte posterior del AlphaShield™ para seleccionar el modo de seguridad preferido. La primera posición seleccionable es el **modo Manual**. Proporciona un valor fijo del temporizador de inactividad de 15 minutos, seguidos de una desconexión lógica. (Modo recomendado de operación). La segunda posición es el **modo Automático**. El valor del temporizador de inactividad es infinito y AlphaShield™ permanece conectado. La tercera posición seleccionable es el **modo Bloqueo** con un valor de inactividad fijo de 15 minutos y una desconexión fisica.

(6) Operación en modo Manual.

Si selecciona el modo Manual, deberá iniciar manualmente una sesión de desconexión pulsando el botón de conexión del AlphaShield™. Una vez pulsado el botón de conexión, el LED de Conexión se iluminará en color verde para indicar al usuario que está conectado a Internet o a la red. El LED de Conexión siempre indicará el estado de conexión del dispositivo AlphaShield™.

(7) Desconexión inmediata de comunicaciones

Puede realizarse una desconexión inmediata en cualquier momento independientemente del modo seleccionado en el AlphaShield™. Esto puede hacerse pulsando el botón de desconexión situado en la parte superior del dispositivo. Una vez desconectado lógica o físicamente, el LED de conexión se iluminará en rojo para indicar que no puede establecerse una comunicación entre los puertos del dispositivo AlphaShield™. Para restablecer la comunicación, el usuario debe pulsar el botón de conexión situado en la parte superior del dispositivo.

(8) Aviso sobre la desconexión en modo Manual

Después de conectar pulsando el botón de conexión en el modo manual, el LED de conexión permanecerá en color verde permanente si hay actividad de comunicación entre los puertos del AlphaShield™. Si faltan 30 segundos para que finalicen los 15 minutos del valor del temporizador seleccionado manualmente, el LED de conexión empezará a parpadear para indicar una inminente desconexión lógica en 30 segundos. Cuando el LED de Conexión parpadee, el usuario puede ampliar la sesión cliente pulsando el botón de conexión cuando aparezca la ventana de aviso de 30 segundos. Una vez pulsado el botón de conexión, el valor del temporizador se restablece en los 15 minutos preseleccionados y el LED de Conexión volverá al verde fijo indicando una sesión de usuario continua.

(9) Operación en modo Automático

Cuando se selecciona el modo Automático debe iniciarse una sesión de conexión pulsando el botón de conexión. El LED de Conexión se iluminará de color verde fijo para indicar que el AlphaShield™ se encuentra en estado de conexión.

La duración de la conexión es infinita independientemente de la actividad del usuario. Se recomienda encarecidamente que una vez el usuario haya finalizado la sesión en Internet, pulse manualmente el botón de desconexión para originar una desconexión lógica.

(10) LED de Datos de entrada

El LED de Datos de entrada siempre permanece en color verde fijo en una buena conexión de enlace y parpadeará cuando el AlphaShield™ acepte un paquete de datos válido. Bajo condiciones de tráfico normales, parpadeará en color verde. El LED de Datos de entrada parpadeará en ámbar o rojo si recibe paquetes no válidos no destinados al cliente y el AlphaShield™ no los dejará pasar. Si existe un gran número de dichos paquetes, parpadeará en rojo.

(11) LED de Datos de salida

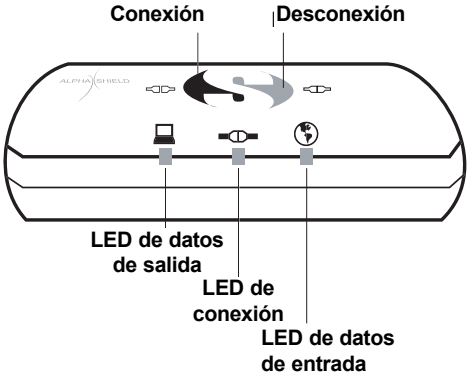
El LED de Datos de salida siempre estará de color verde durante una buena conexión de enlace y parpadeará cuando se transmita un paquete de datos válido a través del AlphaShield™. Parpadeará en verde bajo condiciones de tráfico normales. El LED de Datos de salida parpadeará en ámbar o rojo si recibe paquetes no válidos no destinados a Internet y AlphaShield™ no los autorizará. Si existe un gran número de paquetes ilegales, parpadeará en rojo.

(12) Puerto auxiliar

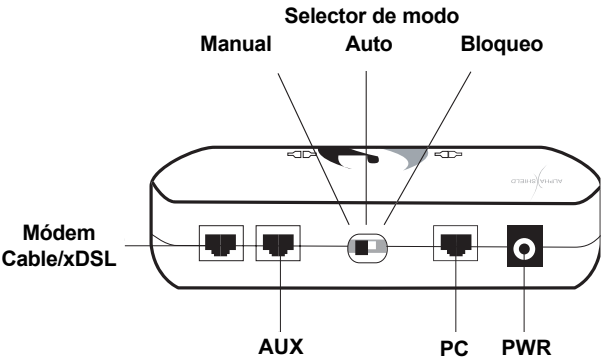
El puerto auxiliar del AlphaShield™ puede utilizarse para proporcionar una conexión con otro dispositivo Ethernet 10Base-T. Aquí podrá conectar un distribuidor, un conmutador o incluso un teléfono VoIP. Este puerto está pensado para dispositivos que no requieran ninguna seguridad.

NOTA: El puerto Auxiliar no proporciona seguridad de ningún tipo.

Vista frontal



Vista posterior



Los indicadores y controles del AlphaShield™ son muy intuitivos y proporcionan una operación de usuario y una interpretación de la red muy fácil. Posee 3 indicadores LED, 2 botones y un conmutador deslizante de selección. Las funciones y los indicadores son los siguientes:

Indicador LED de datos de entrada

El indicador muestra uno de los cinco estados distintos

Sin iluminación indica una mala conexión de enlace entre el módem cable o xDSL y el puerto del módem del AlphaShield™.
La iluminación de color verde fija indica una buena conexión de enlace entre el módem cable o xDSL y el puerto del módem.
Parpadeará en verde cuando encuentre un paquete de datos válido y aceptado por el AlphaShield™ desde el módem cable o xDSL.
Parpadeará en rojo o ámbar cuando encuentre un paquete de datos no válido y descartado por el AlphaShield™ desde el módem cable o xDSL.
Se iluminará en rojo fijo para indicar que el puerto del módem del AlphaShield™ está desconectado físicamente (Modo de Bloqueo).

Indicador LED de datos de salida

El indicador muestra uno de los cinco estados distintos

Sin iluminación indica una mala conexión de datos y de enlace entre el PC del cliente y el puerto de PC de AlphaShield™.
La iluminación de color verde fija indica una buena conexión de enlace entre el PC del cliente y el puerto del PC del AlphaShield™ .
Parpadeará en verde cuando encuentre un paquete de datos válido y aceptado por el AlphaShield™ desde el PC del usuario.
Parpadeará en rojo o en ámbar cuando encuentre un paquete de datos no válido y descartado por el AlphaShield™ desde el PC del usuario.
Se iluminará en rojo fijo para indicar que el puerto del PC del AlphaShield™ está desconectado físicamente (Modo de Bloqueo).

Indicador LED de Conexión/Desconexión
El indicador muestra uno de estos tres estados distintos.

Se ilumina en rojo fijo para indicar que la conexión entre el puerto del PC y el puerto del módem se ha desconectado física o lógicamente. No puede transmitir datos de usuario entre el puerto del PC y el del módem cable o xDSL. El PC se desconecta desde la red. La asignación de IP del ordenador se retendrá o no según la selección del conmutador de modo.

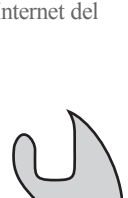
Se ilumina en verde fijo para indicar que la conexión entre el puerto del PC y el puerto del módem está conectada. Sólo se permite el paso entre el puerto del PC y el puerto del módem a los paquetes de datos de sesiones de usuario válidos inspeccionados previamente. Se habilitan AlphaGap™ y RPA. El indicador de conexión/desconexión del AlphaShield™ debe estar de color verde para establecer una conexión con Internet o la red.

Parpadeará en verde para indicar que el valor de 15 minutos para el temporizador de inactividad para la desconexión lógica o física inminente está a punto de exceder. Esto significa que no ha habido ninguna actividad de sesión de usuario durante el valor citado y faltan 30 segundos para que la conexión de la sesión actual se desconecte de forma lógica o física. Sólo la actividad del usuario, por ejemplo hacer clic en un enlace de web o pulsar el botón de conexión situado en la parte superior del Alphashield™, restaurarán el temporizador y mantendrán la sesión de usuario.

Botón de Conexión
Se utiliza para restablecer una conexión nueva después de una desconexión lógica o física. El botón de conexión del AlphaShield™ funciona en el **modo Manual, Automático y de Bloqueo.**

En modo Manual, el botón de conexión debe pulsarse para restablecer una conexión lógica después de una desconexión. En modo manual, la desconexión lógica es debido a que el valor del temporizador de inactividad se ha excedido o a que el usuario ha pulsado el botón de desconexión manualmente. El modo de bloqueo proporciona la misma funcionalidad, excepto con una desconexión física.
En modo Automático, no existe la función del temporizador de desconexión de inactividad. Las conexiones no exceden un tiempo establecido y deben desconectarse manualmente pulsando el botón de desconexión al finalizar la sesión de Internet del usuario.

Botón de Desconexión



El botón de desconexión desconectará lógica o físicamente (según la selección de modo del usuario) cualquier sesión de usuario en proceso actualmente. El botón de desconexión del AlphaShield™ funciona en modo Manual, Automático y de Bloqueo.

El botón de desconexión proporcionará una desconexión lógica o física inmediata después de ser pulsado. El usuario puede pulsar este botón en cualquier momento para invocar una desconexión de sesión. Esto puede hacerse si los LED de Datos de Entrada y de Salida muestran una excesiva actividad de intrusión.

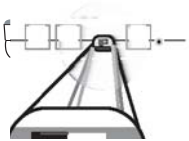
NOTA: Independientemente del modo utilizado, se recomienda que el usuario pulse el botón de desconexión cuando haya terminado su actividad en Internet o en la red. Esto proporcionará un mayor nivel de seguridad. En los modos Manual y de Bloqueo, se desconectará al final de todas formas.

Mode Switch Selector
The slider switch provides 3 user selectable modes of functionality for the AlphaShield™. Each mode will provide a different level of computer security and user convenience.

The first slide position selects the **manual mode** with an inactivity and logical disconnect timer value of 15 minutes. (In this mode the AlphaShield™ will retain the current IP address assignment from the Internet Service Provider.) This is the recommended and default setting for AlphaShield™.

The second slide position selects the **auto mode** with an inactivity disconnect timer value that is infinite. There is no disconnection. (In this mode the AlphaShield™ will retain the current IP address assignment from the Internet Service Provider).

The third slide position selects the **lockout mode** with an inactivity and physical disconnect timer value of 15 minutes. (In this mode the AlphaShield™ will release the current IP address assigned from the Internet Service provider).



El AlphaShield™ proporciona seguridad mediante uno de los tres modos de operación seleccionables siguientes.

El **Modo Manual** proporciona al usuario un nivel de seguridad óptimo y es el modo recomendado y el predeterminado. Proporciona un valor de 15 minutos para el temporizador de inactividad fijo, seguido de una desconexión lógica. En el **Modo Manual**, el AlphaShield™ retiene la dirección IP asignada antes y después de volver a conectarse.

El **Modo Automático** proporciona un gran nivel de seguridad y más comodidad para los usuarios. Posee un valor de temporizador de inactividad infinito y el AlphaShield™ permanece conectado. El **Modo Automático** elimina la intervención física necesaria en el **Modo Manual** para restablecer una sesión de usuario. En este modo, el Alphashield™ retiene la dirección IP asignada después de una desconexión invocada manualmente. En el **Modo Automático** se recomienda que una vez el usuario haya finalizado su sesión de Internet, pulse manualmente el botón de desconexión para originar una desconexión lógica.

El **Modo de Bloqueo** proporciona al usuario el mayor nivel de seguridad disponible en el AlphaShield™. Proporciona un valor de temporizador de inactividad fijo de 15 minutos, seguido de una desconexión física. En el **Modo de Bloqueo**, el AlphaShield™ no retiene la dirección IP asignada después de la desconexión. El **Modo de Bloqueo** desconecta físicamente el ordenador de la red y asegura que no se transmitirá ningún paquete a través del AlphaShield™. Este modo sólo debe utilizarse si es absolutamente necesario.

Los **Modos Manual, Automático y de Bloqueo** todos utilizan la característica de seguridad **AlphaGap™**, junto con las tecnologías **RPA™** e **IP Stealth Technology™**.

Nota: Software antivirus

El dispositivo AlphaShield™ **no elimina** la necesidad de software antivirus en el sistema operativo del cliente. Los dispositivos de seguridad no pueden detectar virus destinados al cliente de una sesión de usuario válida. Los virus también pueden entrar en el sistema del cliente a través del equipo periférico, como por ejemplo unidades de disquetes con un disquete contaminado instalado. Independientemente de si el dispositivo de seguridad está instalado o no, siempre es necesario un software antivirus.

Nota: Tenga siempre una versión actualizada de un software antivirus instalada en el sistema operativo del cliente.

Si actualmente no posee ningún paquete de software antivirus instalado en el PC, **le recomendamos encarecidamente** que utilice el AlphaShield™ en **Modo Manual**. Esto mitigará la posibilidad de que virus tipo troyanos inicien transmisiones desde el lado de usuario de la red mientras se deja el PC desatendido.

			Estatus del Alphashield™
Inactivo	Inactivo	Inactivo	AlphaShield™ no recibe alimentación (Compruebe el adaptador de alimentación).
Rojo	Rojo	Rojo	AlphaShield™ se encuentra en el modo de desconexión física.
Verde	Verde	Verde	AlphaShield™ se encuentra en el Modo de Conexión y está funcionando.
Verde	Rojo	Verde	AlphaShield™ se encuentra en el modo de desconexión lógica.
Verde	V/P	Verde	Faltan 30 segundos para que Alphashield™ se desconecte lógica o físicamente.
Inactivo	V/R	Inactivo	AlphaShield™ no está conectado a ningún puerto de interfaz.
Inactivo	V/R	Verde	AlphaShield™ no está conectado al ordenador.
Verde	V/R	Inactivo	AlphaShield™ no está conectado al módem xDSL o cable.
R/A/P	Verde	Verde	AlphaShield™ está descartando paquetes de datos de salida del ordenador.
Verde	Verde	R/A/P	AlphaShield™ está descartando paquetes de datos de entrada de Internet.
V/P	Verde	Verde	AlphaShield™ está enviando paquetes de datos de salida válidos.
Verde	Verde	V/P	AlphaShield™ está recibiendo paquetes de datos de entrada válidos.

P = Parpadeante
R = Rojo
V = Verde
A = Ámbar
R/A/P = Rojo o Ambar parpadeante
V/P = Verde parpadeante

Selección de modo usuario	Tiempo de inactividad	Método de desconexión	Dirección IP ordenador	RPA habilitado	AlphaGap™ habilitado	IP Stealth activo
Modo manual *(Predeterminado)	15 min. Botón de desconexión	Lógico	Retenida	Sí	Sí	Sí
Modo automático	Ninguno Botón de desconexión	Ninguno Lógico	Retenida	Sí	Sí	Sí
Modo de bloqueo	15 min. Botón de desconexión	Físico	Retenida	Sí	Sí	Sí

Valores predeterminados de inicio del AlphaShield™

AlphaShield™ se iniciará en un estado de desconexión lógica o física según la selección del conmutador de modo.

Modo Manual/Automático
En el modo manual o automático, el AlphaShield™ se iniciará de forma predeterminada en modo de desconexión lógica.

Modo de Bloqueo
En el modo de bloqueo, el AlphaShield™ se iniciará de forma predeterminada en el modo de desconexión física.

Resolución de problemas

El AlphaShield™ no se enciende ¿Por qué?

Asegúrese de que está utilizando el adaptador de alimentación de pared enviado con el AlphaShield™ y no ningún otro (9 voltios CC 300 mA central positiva).
Asegúrese de que la alimentación es de 110 voltios CA o 220 voltios CA. En Norteamérica, 110 VCA.
Si se cumplen todos estos requisitos, puede que el adaptador sea defectuoso.

Cuando conecto el AlphaShield™ al módem xDSL o cable, el LED de estado de enlace de datos de entrada no se enciende. ¿Por qué?

Asegúrese de que el módem xDSL o cable recibe alimentación y está encendido.
Compruebe que el cable de red RJ-45 es una conexión directa y no otra variación.
Asegúrese de que el puerto del módem del AlphaShield™ no está conectado al puerto de red del ordenador.
Aunque el cable sea del tipo correcto, podría ser defectuoso. Sustitúyalo por un cable de red RJ-45 directo nuevo.

Cuando conecto el AlphaShield™ al ordenador, el LED de estado de enlace de datos de salida no se enciende. ¿Por qué?

Asegúrese de que el ordenador recibe alimentación y está encendido.
Compruebe que el cable de red RJ-45 es una conexión directa y no otra variación.
Asegúrese de que la Tarjeta de interfaz de red del ordenador no es una tarjeta Fast Ethernet 100 Mbps fija que no sea capaz de conmutar o gestionar automáticamente a 10 Mbps.

Compruebe que el puerto del ordenador de AlphaShield™ no esté conectado al puerto RJ-45 del módem xDSL o cable.
Asegúrese de que ha enchufado el conector RJ-45 a una Tarjeta de interfaz de red del ordenador y no a otro tipo de tarjeta periférica.
Si se cumplen todos los requisitos anteriores, puede que el cable sea defectuoso. Sustitúyalo por otro cable de red RJ-45 directo.

El LED de Conexión siempre está en verde fijo. ¿Por qué?

Se ha seleccionado el modo automático en la parte posterior de la unidad. Esta indicación verde fija es normal en este modo y se ignora el tiempo excedido de desconexión lógica de 15 minutos. El alphaShield™ permanece conectado y proporciona seguridad mediante las tecnologías AlphaGap™ y RPA hasta que se pulse manualmente el botón de desconexión.

Es imposible realizar una conexión a Internet y los LED de conexión y datos están de color rojo fijo. ¿Por qué?

Si AlphaShield™ se encuentra en el modo de bloqueo, esta situación es normal. En este modo, AlphaShield™ ha desconectado físicamente el ordenador de la conexión de red y no permitirá ninguna comunicación. Este modo sólo debe utilizarse si el usuario requiere medidas de seguridad extremas. Si el usuario no accede a Internet durante un largo período de tiempo o deja el ordenador desatendido y no desea que se establezca ninguna comunicación entre el ordenador y el proveedor ISP, se recomienda este modo.

Los LED de Datos de salida y de entrada no se iluminan en verde y no es posible la comunicación. ¿Por qué?

Verifique que no se hayan intercambiado el cable del ordenador y el de red en el AlphaShield™. El ordenador debe estar conectado al puerto del PC y el xDSL o Cable deben conectarse en el lado del módem. Si están intercambiados, el AlphaShield™ no funcionará.

El LED de conexión rojo se enciende con demasiada frecuencia. ¿Por qué?

AlphaShield™ se encuentra en modo manual o de bloqueo y el usuario no está creando la suficiente actividad para restaurar el temporizador de desconexión por inactividad. Esta situación es normal en el modo manual o de bloqueo si el usuario no está utilizando la conexión con Internet. El LED de conexión proporcionará un aviso de 30 segundos, haciendo parpadear el color verde antes de la desconexión. Se volverá rojo cuando se realice una desconexión lógica o física.

El LED de conexión permanece en color verde en modo manual ¿Por qué?

El LED de conexión permanecerá en color verde en modo manual si el temporizador de sesión de conexión no se ha excedido o si está detectando actividad del usuario cliente. Si el cliente está cargando o descargando un archivo grande que excede el valor del temporizador de inactividad, el LED de conexión permanecerá en verde. El AlphaShield™ continuará conectado y no desconectará al cliente hasta que haya finalizado la transmisión de archivos de datos y el valor del temporizador se exceda sin actividad de transmisión. Este es el funcionamiento normal de AlphaShield™ cuando se encuentre en modo manual o de bloqueo.

El AlphaShield™ no funciona cuando me conecto al hub (distribuidor) o al conmutador. ¿Por qué?

El dispositivo AlphaShield™ es un dispositivo 10Base-T y debe conectarse a un hub o a un conmutador que pueda detectar automáticamente o conmutar a 10Base-T. Si el hub o el conmutador están fijos en 100Base-T, AlphaShield™ no funcionará.

Las sesiones de usuario deben restablecerse después de una desconexión lógica o física. ¿Por qué?

El dispositivo AlphaShield™ contiene un mapa de memoria de sesiones válidas de usuarios válidas concurrentes mientras está conectado a Internet. Cuando se realiza una desconexión lógica o física, manual o automáticamente, la tabla de mapas de IP se elimina. Todas las sesiones de usuarios deben restablecerse después de una desconexión lógica o física, reconectándolas y activándolas de nuevo.

Sólo un ordenador funciona con el dispositivo AlphaShield™. ¿Por qué?

El AlphaShield™ proporciona una correlación de direcciones IP a conexiones de ordenador una a una. Deberá poseer una dirección asignada para cada ordenador conectado en el lado del puerto de PC protegido del AlphaShield™. Este no utiliza ningún tipo de Conversión de direcciones de red.

P: ¿Cuándo se encuentre en modo automático, aún puedo tener una desconexión lógica?

R: Sí. Cuando AlphaShield™ se encuentra en modo automático, la conexión del ordenador utiliza AlphaGap™ , Real Time Packet Authorization (RPA) e IP Stealth. Cuando haya terminado o abandone el ordenador momentáneamente, pulse el botón de desconexión y AlphaShield™ desconectará el ordenador de forma lógica. Se iluminará un LED (indicador luminoso) de desconexión de color rojo.

P: ¿Puedo conmutar de modo automático a modo manual durante una sesión de conexión?

R: Sí. Si está cargando o descargando un archivo grande y no se encuentra delante del ordenador cuando finalice la transferencia del archivo, pero desea que AlphaShield™ se desconecte de forma lógica al finalizar la transferencia, cambie del modo manual al modo automático durante la transferencia de archivos. Una vez haya terminado la transferencia de archivos, se habrá excedido el tiempo de inactividad y se producirá la desconexión lógica de AlphaShield™. También puede seleccionar el modo de bloqueo si desea una desconexión física.

P: ¿Necesito un software antivirus en mi ordenador aunque tenga un dispositivo AlphaShield™ conectado en línea con mi sistema?

R: Sí. AlphaShield™ no puede detectar virus destinados a un cliente de una sesión de usuario válida. Para proteger el sistema operativo y mitigar posibles troyanos que deseen entrar en el sistema a través de la conexión de red o incluso de un dispositivo periférico, recomendamos encarecidamente la instalación de un paquete antivirus actualizado en la máquina cliente.

P: ¿Puedo tener activo AlphaGap™, RPA e IP Stealth para mi ordenador y aún tener otros dispositivos operativos?

R: Sí. Hay un puerto auxiliar disponible en AlphaShield™ activo constantemente pero que no proporciona seguridad. Este puerto puede utilizarse para teléfonos VoIP, conmutadores externos, distribuidores (hubs) o cualquier otro dispositivo IP 10Base-T que no necesite ningún tipo de seguridad.

P: ¿Puedo utilizar el puerto auxiliar como puerto de prueba?

R: Sí. Si cree que tiene algún problema con el AlphaShield™ actual o no puede establecer una conexión a través del mismo, puede conectar el cliente al puerto Aux temporalmente para confirmar que no haya ningún problema con el AlphaShield™. Si el ISP o proveedor de cable sugiere que desactive todos los dispositivos mientras se configura la conexión, conecte el PC al puerto Aux mientras dura la prueba.

NOTA: Cuando termine la prueba o el procedimiento de configuración, recuerde volver a establecer la conexión en el puerto de PC adecuado.

P: ¿Puedo conectar más de un ordenador al dispositivo AlphaShield™?

R: Sí. Si desea conectar más de un ordenador al dispositivo AlphaShield™, deberá conectar el distribuidor o el conmutador al puerto de PC protegido del dispositivo AlphaShield™. También se recomienda cambiar el dispositivo a modo automático. Deberá tener una asignación de dirección IP de la compañía telefónica o de cable local para cada ordenador conectado a AlphaShield™.

P: ¿Puede alguien entrar en el código operativo residente en AlphaShield™?
R: No. El programa operativo de seguridad propiedad de AlphaShield™ reside en memoria y es imposible alterarlo desde los puertos del PC o de red del dispositivo.

P: ¿AlphaShield™ proporciona NAT para una sola operación IP?
R: No. AlphaShield™ no da soporte a múltiples operaciones cliente a través de NAT, pero da soporte a un número igual de direcciones IP de conexiones de ordenador a través del AlphaShield™.

P: ¿Puede mi dispositivo AlphaShield™ ser detectado y hacérsele la prueba Ping desde Internet cuando esté en modo de conexión o desconexión?
R: No. AlphaShield™ no actúa como una pasarela (gateway) o un direccionador convencionales y no tiene asociada ninguna asignación de dirección IP de ningún tipo. AlphaShield™ permanece invisible en Internet, Intranet o cualquier red conectada.

P: Si se conoce la dirección IP del ordenador, ¿puede hacerse la prueba Ping?
R: No. AlphaShield™ ocultará la dirección IP del ordenador, y no responderá a ninguna solicitud de prueba Ping del exterior. Se descartarán los paquetes ICMP para el mandato Ping.

P: ¿Funciona AlphaShield™ con programas como MSN Messenger o ICQ?
R: Sí. Si usted es el que inicia la sesión de MSN Messenger o ICQ. Sin embargo, si usted es el destinatario de una solicitud MSN Messenger o ICQ, AlphaShield™ denegará el acceso al PC ya que estos programas permiten el acceso no autorizado, lo que puede originar intrusiones fatales en los ordenadores. AlphaShield™ no permitirá la comunicación de igual a igual.

P: ¿Proporciona AlphaShield™ seguridad entre ordenadores en la LAN?
R: Sí. AlphaShield™ proporciona seguridad entre su ordenador y otros ordenadores de la red de área local. Para proporcionar seguridad a todos los clientes de la red local, deberá tener un dispositivo AlphaShield™ por ordenador.

P: ¿AlphaShield™ retendrá mi dirección IP asignada por el proveedor ISP después de una desconexión lógica?
R: Sí. Cuando AlphaShield™ se encuentra en estado de desconexión lógica con el LED de Conexión en color rojo, retiene la dirección IP asignada actualmente por el ISP. Tanto si se encuentra en el modo Manual como en el Automático, AlphaShield™ tiene capacidad para retener la dirección IP asignada durante y después de una desconexión lógica.

P: ¿AlphaShield™ retiene sus valores de configuración después de un corte de fluido eléctrico?
R: Sí. AlphaShield™ se encenderá y funcionará sin ningún cambio después de un cortocircuito. Sin embargo, por defecto, entrará en estado de desconexión de seguridad cuando se restablezca la alimentación. Se activará en un estado de desconexión lógica o física, según la posición seleccionada en el conmutador de modo.

P: ¿Puedo utilizar AlphaShield™ en mi oficina para obtener seguridad?
R: Sí. Puede utilizarse en un entorno de oficina sólo si el distribuidor o el conmutador utilizados tienen la capacidad de detectar y conmutar a una conexión 10 Base-T. Si la conexión sólo es una conexión 100Base-T, AlphaShield™ no funcionará.

P: ¿Puedo realizar una conexión utilizando PC Anywhere o VNC o cualquier programa de acceso remoto a través de un cliente remoto utilizando el dispositivo AlphaShield™?

R: No. Los programas de acceso remoto no funcionarán o no permitirán la conexión desde la red externa a través de AlphaShield™ con el PC.

P: ¿Puedo "teleconmutar" y realizar una conexión remota utilizando PC Anywhere o VNC desde el puerto del ordenador al exterior a través de AlphaShield™?

R: Sí. Si desea realizar una conexión remota desde el lado cliente o del ordenador de AlphaShield™ a un sitio remoto utilizando software de aplicación remota, como por ejemplo PC Anywhere, AlphaShield™ permite este tipo de conexión. El otro extremo no debe tener ningún dispositivo de seguridad, como por ejemplo AlphaShield™ en línea con el PC asociado.

P: ¿Puedo tener múltiples iteraciones del explorador ejecutándose en múltiples sesiones?

R: Sí. AlphaShield™ realiza un seguimiento de todas las sesiones concurrentes iniciadas en la parte cliente de la red y las considera sesiones de usuario válidas. Cuando se produce una desconexión, debido a un tiempo excedido o a una desconexión manual, se pierden todas las conexiones de sesión actuales y deben restablecerse después de pulsar el botón de conexión.

P: ¿Funcionará AlphaShield™ detrás de un firewall existente para proporcionar seguridad adicional?

R: Sí. Muchos firewalls son difíciles de configurar y quizás no estén proporcionando la seguridad esperada. AlphaShield™ asegurará un alto grado de seguridad, independientemente del lugar donde se haya instalado dentro de la topología de red.

P: ¿Puede AlphaShield™ funcionar en asignación de dirección IP estática o dinámica?

R: Sí. AlphaShield™ puede dar soporte a direcciones IP estáticas o dinámicas, siempre y cuando el cliente haya sido configurado correctamente para el acceso asignado. Cada ordenador tendrá o se le asignará una dirección IP para conectarse a la red.

P: ¿Puede ignorarse la desconexión lógica o física en modo manual si un hacker entra en AlphaShield™?

R: No. Una vez excedido el valor del temporizador de inactividad o si se ha pulsado el botón de desconexión para crear una desconexión lógica, ningún software ni iw 1o posible, tantolor d31 rtolel cliencomoloelca,purloea

P: ¯r sofunciede AlphaShield™ funces63n informe63n dl clies231?R: SEl63ngic

P: ¯ermituede AlphaShield¯se ennsmisnación 3n mexcslie 3nSEC paraa o

R: Sí. AlphaShield¯nceen if55sise ennsmisnación paqueies63n do mtosca,

P: ¿Puedo utilizar cualquier sistema operativo con AlphaShield™?
R: Sí. AlphaShield™ funcionará con cualquier sistema operativo, siempre y cuando el protocolo de red seleccionado sea TCP/IP.

P: ¿Puedo utilizar un servidor proxy delante del dispositivo AlphaShield™ para proporcionar múltiples asignaciones IP a varios ordenadores?
R: Sí. Aunque AlphaShield™ está pensado para uso doméstico, puede utilizar un servidor proxy en múltiples conexiones IP NAT, para que puedan conectarse y protegerse ordenadores adicionales.

P: ¿Puedo conectar AlphaShield™ si tengo un módem interno xDSL en el ordenador?
R: No. AlphaShield™ está diseñado para que funcione situándolo entre el módem xDSL y el ordenador cliente. Si posee un módem xDSL interno, no podrá conectar AlphaShield™. Necesita un módem externo.

P: ¿Puedo conectar AlphaShield™ si la Tarjeta de interfaz de red de mi ordenador es una tarjeta fija Fast Ethernet 100 Mbps?
R: No. AlphaShield™ debe conectarse a una Tarjeta de interfaz de red que pueda cambiar automáticamente a una velocidad de datos de 10 Mbps. Algunas tarjetas rápidas Ethernet dan soporte a la conmutación automática a 10 Mbps. Es preferible tener instalada una tarjeta de interfaz de red 10/100 Mbps en el ordenador cliente.

El fabricante otorga a Alphashield™ una garantía exclusiva de un año en materiales y mano de obra desde la fecha de compra. El AlphaShield™ proporcionará años de seguridad de red y un funcionamiento sin problemas si se conecta y se utiliza correctamente tal como se indica en las instrucciones de este manual. Si experimenta algún problema con el AlphaShield™, consulte la sección de resolución de problemas de este manual.

En el caso de que el AlphaShield™ sea defectuoso, la responsabilidad del fabricante se limitará a sustituir o reparar el producto defectuoso siempre y cuando se cumplan los siguientes requisitos:

- El producto no se ha reparado ni alterado sin el consentimiento por escrito del fabricante.
- El producto no se ha dañado debido a un mal uso, un mantenimiento inadecuado, descuido o daños físicos.

Esto no implica ninguna otra garantía o condición y el fabricante no será responsable bajo ningún concepto de los daños originados por de la utilización del dispositivo AlphaShield™.

Para obtener servicio técnico, póngase en contacto con el fabricante en los números y direcciones siguientes:

E-mail: tech-support@saafnet.com
Teléfono: 1-866-7222-3638 o 1-604-435-0700
1-8666-Saafnet
Fax: 1-604-435-0702

Recuerde que no podemos aceptar material sin el número RMA (Autorización de devolución de material) correspondiente. El número RMA puede obtenerlo poniéndose en contacto con Saafnet International Inc. antes de enviar la unidad.

Limitación de responsabilidades y daños

Ni, AlphaShield Inc., ni sus agentes, empleados, proveedores, concesionarios y demás representantes autorizados quedarán sujetos a responsabilidad alguna en relación con el producto por daños indirectos, incidentales o especiales, inclusive la pérdida de información, operaciones comerciales o beneficios, ni con cualesquiera asuntos conexos que surgieren por razones contractuales, negligencia, responsabilidad objetiva u otras cuestiones litigiosas

Marca registrada

AlphaShield™, AlphaGap™, AlphaGuardian™ y el logo de AlphaShield™ son marcas registradas pendientes y son marcas comerciales de Saafnet International Inc. en Canadá, Estados Unidos y otros países. Se ha realizado un gran esfuerzo para que la información que aparece en este manual sea precisa. Saafnet International Inc. no se responsabiliza de ningún error de impresión que pudiera aparecer. La información de este documento está sujeta a cambios sin previo aviso.

Patentes

El producto al que acompaña este documento está protegido por una o más patentes y patentes pendientes de EE.UU. o del extranjero llevadas a cabo por AlphaShield Inc.

Restricciones

Bajo ningún concepto se le permite a usted ni a ninguna otra empresa descompilar, desmontar, utilizar técnicas de ingeniería o intentar reconstruir o descubrir ningún código fuente ni las ideas o algoritmos subyacentes del software.

Documentación

Ninguna parte de este documento puede reproducirse ni retransmitirse, ni electrónica ni mecánicamente, sea cual sea el objetivo sin el permiso expreso por escrito de Saafnet International Inc. Bajo ley, reproducir incluye traducir a cualquier otro idioma o formato.

Entre empresas, Saafnet International Inc. mantiene la titularidad y la propiedad de todos los derechos de propiedad respecto al software de sus productos. El software y el firmware están protegidos por las leyes de copyright de Estados Unidos y lo estipulado en el Tratado Internacional. Por consiguiente, deberá tratar el software y el firmware como cualquier otro material de copyright.

Aviso de copyright

Saafnet International Inc. le autoriza a copiar materiales publicados por Saafnet sólo para uso no comercial dentro de su empresa para soporte a productos Saafnet. Cualquier copia realizada de este material debe poseer los avisos de propiedad y de copyright con el mismo formato que en el original.

La única parte sustituible del AlphaShield™ es el adaptador de alimentación. Si se rompe o se daña, puede sustituirse por un adaptador de alimentación de pared de 9.0 voltios CC estándar. El voltaje debe ser de 9.0 VCC @300 mA de polaridad positiva y central. Este adaptador de alimentación puede adquirirse en tiendas de electrónica y distribuidores. Si necesita un nuevo adaptador, puede comprarlo a Radio Shack. El tamaño del enchufe debe ser de 3,4 mm DE x 1.3 mm DI. En Norteamérica, puede comprarse el siguiente adaptador de alimentación.

. Adaptador de alimentación de Radio Shack Número de pieza 273-1767ª
. Adaptador Radio Adaptaplug Número de pieza 273-1711

AlphaShield™ requiere una polaridad positiva para proporcionarla al conductor central del enchufe de alimentación. Asegúrese de que conecta el enchufe del adaptador correcto para proporcionar la alimentación adecuada a AlphaShield™.

También puede obtener un adaptador de alimentación universal de sustitución solicitándolo directamente a Saafnet International Inc. Saafnet International le cobrará un importe de $11.99 U.S., previo pago, por el adaptador de alimentación más cualquier gasto de envío y entrega adicionales.

No utilice ningún otro tipo de adaptador de alimentación que no sea el especificado en este manual. Si no lo hace, puede ocasionar daños permanentes en el Alphashield™ y se invalidará la garantía.

10BASE-T La especificación 802.3 del IEEE (Institute of Electrical and Electronic Engineers) para Ethernet sobre cable coaxial delgado o UTP a 10 Mbps.

100BASE-T Fast Ethernet es una transmisión de la LAN (Red de área local) estándar que proporciona una velocidad de datos de 100 Mbps en cable UTP. La mayoría de dispositivos 100base-T seleccionarán la velocidad automáticamente si se conectan a un puerto 10Base-T.

Acceso remoto a la LAN (Remote LAN Access) Comunicación de datos, como en un entorno empresarial o de campus universitario, en el cual se puede acceder remotamente a las redes mediante redes de telecomunicaciones públicas.

ADSL Asymmetric Digital Subscriber Line es un nuevo método de transmisión a velocidades de hasta 7 Mbps en una dirección a través de una única línea telefónica de cobre de hasta 640Kbps en la otra dirección.

AlphaGap™ Método de propiedad para desautorizar la transmisión de datos en paquetes, rompiendo la conexión lógica o física entre dos puertos, proporcionando así seguridad garantizada (propiedad de AlphaShield™).

Ancho de banda (Bandwith) Término utilizado para describir la capacidad o cantidad de tráfico (datos, voz o vídeo) que una línea de comunicación concreta es capaz de asumir.

Asimétrico (Asymmetric) Indica que existe una diferencia apreciable de velocidad de datos entre las dos direcciones de un enlace de transmisión.

Ataques Smurf (Smurf Attacks) Ataque de denegación de servicio de un hacker, como por ejemplo enviar un conjunto de mensajes ping de diagnóstico a una lista de servidores IP, que a su vez los enviarán a todas las estaciones de trabajo LAN conectadas y que estas a su vez contestarán. Sin embargo, la dirección de destino muestra la del destino del ataque. El resultado es un conjunto de respuestas que se magnifica varias veces, cerrando de forma eficaz el servidor de destino.

Ataque Teardrop (Teardrop Attack) Ataque que se produce cuando un hacker envía instrucciones por una red intentando colapsar el servidor. Algunas implementaciones del código de reensamblaje de fragmentación TCP/IP no manejan correctamente los fragmentos IP que se solapan. El ataque Teardrop es una herramienta de ataque ampliamente disponible que explota esta vulnerabilidad.

Banda ancha (Broadband) Transmisión de datos a una velocidad normalmente superior a la velocidad T1 (1,5 Mbps). Permite la transmisión de voz, datos y señales de vídeo en un solo medio.

Bits por segundo (bps) (Bits per second) Número de bits que pasa por un punto fijo cada segundo. Unidades utilizadas para la velocidad de transmisión de la información digital.

Caballo Toyano (Trojan Horse) Nombre genérico para un virus o programa de violación de seguridad camuflado como otra cosa, una lista de directorios o un archivo. Un caballo Troyano puede ser software que parezca que está realizando una operación normal, pero contiene una trampa o un programa de ataque.

Cliente/Servidor (Client/Server) Modelo informático de sistema distribuido el cual aporta el poder informático al escritorio, donde los usuarios (clientes) acceden a los recursos desde servidores.

Conectividad (Connectivity) Capacidad de comunicar entre ordenadores y terminales. Puede ser una vía de conexión física o lógica.

Cortafuegos (Firewall) Dispositivo de seguridad (hardware o software) que controla el acceso a y desde Internet a una red local mediante información de identificación.

Datagrama (Datagram) Paquete único de información que se envía como unidad de capa de red a través de un medio de transmisión sin establecer primero un circuito virtual. Los datagramas IP son la unidad primaria de transmisión en redes TCP/IP, como por ejemplo Internet.

Denegación de servicio (DOS) (Denial Of Service) Tipo de ataque nocivo que colapsa la dirección IP de destino con solicitudes. Por ejemplo, realizando la prueba Ping de 400 a 500 veces por segundo.

Desconexión física (Physical Disconnect) Tipo de desconexión que se produce en la capa de red física inhabilitando de forma eficaz todos los mensajes de comunicación en ambas direcciones. Funcionalmente, el circuito está abierto eléctricamente y no puede establecer una vía de comunicación debido a que no hay una conexión.

Desconexión lógica (Logic disconnect) Tipo de desconexión que sólo permite pasar mensajes de la capa de aplicación DHCP entre ordenadores cliente y el servidor DHCP del Proveedor de servicio de Internet. Todos los demás tipos de mensajes están prohibidos y se descartan. En el estado de desconexión lógica, el ordenador del cliente retiene la dirección IP asignada previamente aunque se haya reestablecido la conexión.

Detección automática 10/100 (Auto Detection 10/100) Dispositivo de red, como por ejemplo un Hub o un conmutador, que puede detectar y conmutar a la velocidad fijada del dispositivo conectado al mismo.

Dirección IP (IP direction) Dirección de Internet formada por un número exclusivo de cuatro partes separadas por puntos, denominado a veces grupo de puntos. Cada una de las partes es un número del 0 al 255. Cada ordenador posee una dirección IP.

Dirección MAC (MAC Address) Media Access Control es una dirección exclusiva asociada con una tarjeta Ethernet.

Direccionador (Router) Dispositivo que realiza direccionamientos y vías de acceso apropiadas para paquetes de datos a través de las redes cuando pasan por una red local o WAN.

Distribuidor (Hub) En entornos de Internet, dispositivo que concentra y combina las señales de múltiples conexiones 10Base-T independientes en un segmento.

DNS El Sistema de nombre de dominio (Domain Name System) es un mecanismo utilizado en Internet o Intranet para convertir nombres de ordenadores host en direcciones. DNS permite a los ordenadores host que no estén directamente en Internet registrar nombres del mismo estilo. DNS le permite utilizar Internet sin recordar largas listas de números.

DOS distribuido (DDOS) (Distributed DOS) Una denegación de servicio distribuido ataca una dirección IP de destino desde múltiples recursos simultáneamente, colapsando el servidor. Los ataques DDOS parecen tráfico de Internet válido, ya que no aparece ninguna dirección IP como el origen del ataque.

DSL Digital Subscriber Line es otro nombre para un canal ISDN BRI. Funciona en la interfaz de velocidad básica con dos canales de conmutación de circuito de 64 Kbps y un canal de conmutación de paquetes de 16 Kbps.

Emisión (Broadcast) Paquete de datos que se envía a cada dispositivo de una red.

Enlace (Link) Conexión física entre dos nodos de una red. Puede estar formado por un circuito de comunicación de datos o por una conexión de canal directo (cable). La señal luminosa de un LED indica que se ha establecido la conexión.

Explorador (Browser) Término general para software cliente de WWW. Netscape, Internet Explorer y Mosaic son exploradores conocidos.

Exploración de puertos (Port Scanning) Técnica para intentar encontrar puertos TCP o UDP de escucha en un dispositivo IP y extraer de dichos puertos tanta información como sea posible sobre el dispositivo y utilizar la información para entrar en una fecha posterior.

Explorador de Web (Web Browser) Un explorador de web es un software de comunicaciones que permite a un usuario de ordenador "navegar" por la World Wide Web. Le permite seleccionar, recuperar e interactuar con recursos de la Web.

Ethernet Especificación LAN de banda base inventada por Xero Corporation y desarrollada junto con Xerox, Intel y DEC. Las redes Ethernet operan a 10 Mbps utilizando CSMA/CD para ejecutarse sobre un cable coaxial o UTP. Ethernet se ha convertido en una serie de estándares producidos por IEEE, a los que se hace referencia como IEEE 802.3.

Filtrado de paquetes (Packet Filtering) Seguridad establecida mediante la utilización de un grupo de normas para filtros que funciona examinando paquetes IP para permitirles pasar o no. Un direccionador (router) que implemente filtros de paquetes se conoce como direccionador de pantalla o direccionador cortafuegos (firewall router).

FTP File Transfer Protocol es la función básica de Internet que permite transferir archivos entre ordenadores. Puede utilizarlo para descargar archivos desde un ordenador host remoto y para cargar archivos desde el ordenador.

HHTP Hyper Text Transfer Protocol es el protocolo real utilizado por el servidor de la Web y el explorador cliente para comunicarse en la red. Este protocolo se utiliza para enviar documentos por la red.

ICMP Internet Control Message Protocol es un protocolo de Internet a nivel de red que proporciona paquetes de mensajes para informar de errores y demás información relevante para el proceso de paquetes IP. ICMP proporciona un número de funciones de diagnóstico y puede enviar paquetes de error al host. ICMP utiliza el soporte básico de IP y es una parte integral de IP.

IMAP Internet Messaging Access Protocol es un protocolo de correo electrónico de próxima generación candidato a sustituir a POP (Post Office Protocol) para servidores de correo de Internet. IMAP permite a los usuarios crear y gestionar carpetas de correo sobre la WAN, así como escanear cabeceras de mensajes y descargar sólo los mensajes seleccionados. IMAP es la versión actual ratificada.

Internet Control Message Protocol Tipo de paquete de datos utilizado en redes TCP/IP que facilita la transmisión de varios tipos de errores y demás información relacionada con la entrega de paquetes de datos sobre la red.

Intranet Red privada que utiliza software de Internet y estándares.

IP dinámica (Dynamic IP) Una dirección IP dinámica es una dirección IP que cambia periódicamente. Cada vez que usted se conecta a Internet, se le asigna una dirección IP distinta. Esto evita que puedan localizar fácilmente el ordenador u otros dispositivos desde cualquier lugar de Internet.

IP estática Una dirección IP estática es una dirección IP "fija" asignada a un ordenador concreto u a otro dispositivo de una red. La dirección IP no cambia y se asocia con dicho ordenador o dispositivo.

IP ficticias (IP Spoofing) Técnica utilizada para obtener acceso no autorizado a ordenadores, donde el intruso envía mensajes a un ordenador con una dirección IP indicando que dicho mensaje proviene de un host fiable. Para utilizar esta técnica, un hacker debe primero utilizar una variedad de técnicas para encontrar una dirección IP de un host fiable y modificar las cabeceras de los paquetes para que parezca que los paquetes provienen de dicho host. Algunas opciones de direccionadores (routers) y cortafuegos (firewalls) pueden ofrecer protección contra las IP ficticias.

IP Protocolo de Internet. Dirección IP que permite identificar un ordenador en Internet mientras el usuario está en línea.

IPSEC Grupo de medidas de seguridad IP que comprende un protocolo de túnel opcional. Una cabecera de seguridad de carga útil encapsulada cifra el datagrama completo, basándose en el algoritmo de cifrado seleccionado por los implementadores.

ISP El proveedor de servicio de Internet es una organización que proporciona acceso a Internet.

Kbps Los Kilobites por segundo (1000 bits por segundo) son una medida de velocidad de transmisión de datos.

LAN (Local Area Network) La red de área local es la forma mediante la cual una comunidad de usuarios y grupos de trabajo locales pueden compartir información y recursos electrónicamente. Para ello, se utilizan muchos protocolos de comunicación, pero los más conocidos son Ethernet y Red en anillo (Token Ring).

Land Attack Ataque que se produce cuando una persona envía instrucciones a un servidor a través de la red para intentar colapsarlo. El proceso es el siguiente: se engaña al servidor de destino para que intente configurar una sesión TCP consigo mismo. Si la máquina no realiza este tipo de IP ficticia, entra en un bucle cerrado de TCP y debe reiniciarse.

Latencia (Latency) En un entorno de red, la diferencia de tiempo entre el momento en que se formula una solicitud de envío de datos y el momento en que la transmisión empieza realmente.

Marcación (Dialup) Tipo de comunicación establecida por una conexión de circuito conmutado mediante la red telefónica.

MIB Management Information Base es una base de datos de información del rendimiento de la red que se almacena en un agente de red para acceder a la misma mediante una estación de gestión de redes (Network Management Station). Los dispositivos como un NIC, un distribuidor (hub), un conmutador (switch) y un direccionador (router) saben cómo responder a un conjunto estándar de solicitudes.

Módem cable (Cable Modem) Módem diseñado para utilizarlo en un circuito de cable coaxial de TV. Generalmente proporciona conectividad de Internet asimétrica de alta velocidad.

NAT (Network Address Translation) La conversión de direcciones de red es un estándar de Internet que permite a una red de área local utilizar un conjunto de direcciones IP para tráfico interno y un segundo grupo de direcciones IP para tráfico externo. Esto permite a una empresa proteger las direcciones internas de Internet pública. NAT convierte las direcciones locales internas en direcciones IP exclusivas antes de enviar paquetes a la red externa.

Negociación automática (Auto Negotiation) Componente integral pero opcional de 100Base-T Fast Ethernet estándar. Determina la velocidad operativa de los dispositivos de red conectados (10 Mbps o 100 Mbps).

NIC (Network Interface Card) La tarjeta de interfaz de red es una placa de circuito instalada en un PC que proporciona la interfaz entre un PC y la red con la que se comunica.

Paquete (Packet) Agrupación de información lógica que incluye una cabecera y datos de usuario (normalmente). A través de la red y de una unidad integral, se conmuta una secuencia continua de dígitos binarios de información.

Paquete ARP (ARP Packet) Un paquete ARP funciona en la misma capa aproximadamente que IP. Se comunica con los servicios de enlace de datos proporcionados por el medio físico y como tal, ARP es un protocolo distinto a un IP (y es identificado de forma independiente por cualquier red que categorice los protocolos existentes en las tramas de niveles bajos y soporta ARP directamente).

Pasarela (Gateway) Es una entrada y una salida a una red de comunicaciones. Una pasarela intercepta y dirige señales electrónicas de una red a otra. En redes de datos, las pasarelas son normalmente un nodo en ambas redes que conecta dos redes de lo contrario incompatibles.
Pila de protocolos (Protocol Stack) Conjunto de módulos de software interrelacionados (apilados) que forman un conjunto de conversiones de comunicación. Por ejemplo, TCP/IP es un protocolo formado por varios protocolos separados, como TCP, UDP, IP, ICMP y otros.

Ping Método mediante el cual se envía un paquete ICMP a través de la red TCP/IP a una dirección concreta y vuelve para confirmar que puede llegarse a un sitio concreto a través de la red.

Plug and Play (Enchufar y listo) Dispositivo que se instala sin la necesidad de ajustar interruptores o configuraciones y que posee la capacidad de identificarse a sí mismo y a los recursos que necesita.

POP3 Post Office Protocol es un protocolo de Internet que permite a un usuario leer correo electrónico de un servidor de correo.

Proveedor de acceso (Access Provider) Organización que proporciona y mantiene servicios de red para los suscriptores.

Puente (Bridge) Dispositivo utilizado para conectar a segmentos de una red y permitir la transmisión de datos de segmento a segmento. Los puentes funcionan en la capa 2 del modelo OSI. Un puente examina todos los paquetes de su interfaz, y filtra y envía un punto de dirección de destino de la capa 2 de la trama.

Puerto (Port) Punto de acceso de software a un host. Los hosts tienen múltiples puertos y daemons que escuchan un puerto o puertos específicos para la conexión desde clientes.

RJ-45 Conectores estándares de ocho cables utilizados en redes 10Base-T y 100Base-T IEEE 802.3.

RPA La autorización de paquetes en tiempo real (Real-Time Packet Authorization) es un proceso de inspección de paquetes en tiempo real de autoaprendizaje que sólo permite la entrada de información verificada, solicitada específicamente por el usuario original. (Tecnología propiedad de AlphaShield™)
Servidor DHCP (DHCP Server) El protocolo DHCP es un protocolo TCP/IP que permite a los PC y a las estaciones de trabajo obtener direcciones IP temporales o permanentes (fuera de un sondeo) desde un servidor administrado centralmente. DCHP permite a un servidor asignar dinámicamente direcciones IP a estaciones de trabajo simultáneamente.

Servidor Proxy (Proxy Server) Un proxy es una aplicación que se ejecuta en una pasarela que transmite paquetes entre un cliente fiable y un host no fiable. Puede proporcionar características adicionales como puesta en antememoria, seguridad en Internet y consolidación de direcciones IP.

Servidor WWW Ordenador que envía datos al explorador que los ha solicitado. Algunos servidores WWW pueden realizar funciones personalizadas, como por ejemplo CGI.

SLIP Serial Line Internet Protocol es un método de envío a TCP/IP mediante una línea serie, especialmente utilizando conexiones de marcación. Uno de los dos métodos principales de proporcionar Internet bajo solicitud a consumidores y a otros usuarios de bajo volumen.

SMTP El protocolo de intercambio de correo electrónico estándar de Internet.

SNMP Simple Network Management Protocol es un software de gestión de red de capas de aplicación. SNMP es ampliamente utilizado en redes TCP/IP para acceder a información MIB. SNMP pasó a ser un estándar TCP/IP en mayo de 1990.

T1 Recurso de transmisión digital que funciona con un ancho de banda nominal de 1,544 Mbps. El sistema de transmisión digital T1 es el principal sistema de comunicación digital en Norteamérica.

Tarjeta Ethernet (Ethernet Card) Placa de circuito impreso que se enchufa en un ordenador para permitir que éste se conecte a la red.

TCP/IP Transmission Control Protocol/Internet Protocol es un protocolo de transporte de extremo a extremo orientado a conexión, dúplex y fiable que se ejecuta sobre IP.

Teletrabajador (Telecommuter) Persona que realiza un trabajo desde casa conectado a la oficina mediante un sistema informático equipado con telecomunicaciones.

Telnet Programa que le permite conectarse a otros ordenadores de Internet. Proceso mediante el cual una persona que utiliza un ordenador puede conectarse a otro ordenador de una ubicación alternativa. Telnet es el protocolo host remoto de terminal desarrollado por ARPAnet. Utilizando Telnet, usted puede trabajar desde el PC como si fuera una terminal conectada a otro ordenador mediante una conexión de cable física.

TFTP Trivial File Transfer Protocol es una versión simplificada de FTP el cual transfiere archivos pero no proporciona protección de contraseña ni posibilidad de directorios de usuario. Pertenece a la familia TCP/IP de protocolos. TFTP depende del servicio de entrega de datagramas sin conexión, UDP.

Topología Diseño de red física o flujo de datos sobre una red, el cual incluye varios distribuidores u otros dispositivos de red.

UDP User Datagram Protocol es un protocolo TCP/IP que describe cómo llegan los mensajes a los programas de aplicación de un ordenador de destino. UDP es un protocolo de modo sin conexión de capa de transporte que proporciona un modo de datagrama sin secuencia potencialmente no fiable para la entrega de paquetes a un usuario remoto.

Virus Programa de software capaz de copiarse a sí mismo y generalmente capaz de realizar grandes daños en el sistema.

VPN Virtual Private Network es, en términos sencillos, una red de comunicaciones privada que utiliza una red privada distinta a la PSTN como red troncal WAN. Una VPN suele ser una red definida por software que se ejecuta en una red privada compartida y posee el aspecto, la funcionalidad y la utilidad de una red privada dedicada a un precio asequible.

VoIP Voice over IP es una forma de transmisión de datos IP que permite el transporte de paquetes de voz sobre una red IP privada o pública.

WAN Wide Area Network (Red de área amplia) es una red de voz y ordenador mayor que un área metropolitana o una ciudad.

Web Abreviación de World Wide Web de Internet.

xDSL La letra genérica x significa un término para los servicios y equipos Digital Subscriber Line, que incluyen las tecnologías ADSL, HDSL, IDSL y VDSL las cuales proporcionan un ancho de banda extremadamente alto para los cables de cobre de par trenzado que la compañía telefónica despliega por la infraestructura de red telefónica.

Categoría	AlphaShield™
Garantía	Garantía limitada de 1 año
Velocidades de interfaz	Velocidades de enlace de hasta 10 Mbps
Fuente de alimentación	Adaptador de pared CC de 9 VCC 4,5 vatios
Protección de línea ESD	Cada puerto hasta 1500 VCC
Interfaces eléctricas	3 conectores RJ-45 10Base-T IEEE 802.3
Interfaces de red	1 puerto cliente Ethernet 10Base-T protegido
Interfaces de red	1 conexión de módem de puerto Ethernet 10Base-T
Interfaces de red	1 puerto auxiliar 10Base-T no protegido
Configuración de software	Ninguna, dispositivo "plug&play" real
Sistema operativo	Se ejecuta en todos los sistemas operativos (Plataforma agnóstica)
Interfaz de terminal	Control de botones (2 botones)
Reconexión de sesión	Intervención manual (Botón Restaurar)
Retención tras fallo en alimentación	Retiene los valores no volátiles
Dirección IP de dispositivo	Ninguna asignación de dirección IP para dispositivo
Conversión de dirección IP	Ninguna (el dispositivo no proporciona ninguna conversión de dirección)

Número máx. de usuarios	Hasta 10 ordenadores
Conexión de seguridad	Tecnología AlphaGap de dominio de tiempo
Inspección de paquetes	Firewall RPA (Real-Time Packet Authorization)
Protocolos soportados	TCP/IP, FTP, UDP, HTTP, TFTP, IMAP, DNS
Modos de operación	3 modos de operación: manual, automático y de bloqueo
Tiempos de sesión de usuario	Seleccionable por el usuario (2 valores)
Alerta de intrusión	Indicador LED visual en rojo o ámbar
Desconexión instantánea	Intervención manual (Botón)
Conexión física	LED de estado de enlace en puertos 10Base-T
Alimentación al dispositivo	Indicador de alimentación a través del LED de Conexión
Transmisión de datos	Indicadores LED de entrada /salida
Modo de operación	Seleccionable mediante conmutador de múltiples posiciones
Indicador de conexión	Indicador LED de dos colores y dos estados
Temperatura en funcionamiento	De 10ºC a 43ºC (50 a 110 grados F)
Peso	150 gramos

NOTA: El dispositivo AlphaShield™ no posee componentes a los que el usuario pueda dar servicio técnico. Si se abre el dispositivo, se INVALIDARÁ LA GARANTÍA y puede que se originen daños permanentes en los dispositivos electrónicos sensibles a la electricidad estática. Si observa cualquier problema con el AlphaShield™, consulte la sección de resolución de problemas detallados que encontrará en esta guía del usuario.

AlphaShield Inc. garantiza que este producto está libre de defectos y que es totalmente funcional durante un período de 12 meses a partir de la fecha de compra original. AlphaShield Inc. reparará o sustituirá a opción de AlphaShield cualquier unidad, sin coste adicional, durante este período si la unidad está defectuosa por cualquier motivo, siempre y cuando no se deba a un mal uso o abuso o a una mala instalación. AlphaShield Inc. ofrece una garantía adicional de 48 meses que puede obtener registrándose en línea en la dirección www.alphashield.com.

No intente reparar la unidad. Si tiene algún problema, póngase en contacto con AlphaShield Inc. para obtener primero un número RMA antes de enviarlo. Cualquier modificación de la unidad realizada por personal no autorizado por AlphaShield invalidará la garantía.

Si necesita reparar un AlphaShield™, llame a AlphaShield para obtener un número RMA (Autorización de material de retorno) y envíe la unidad defectuosa, a portes pagados, junto con una breve descripción del problema, a la siguiente dirección:

AlphaShield Inc.
5945 Kathleen Street
Burnaby B.C. V5H 4J7
Canadá
ATT.: Departamento de Reparaciones y devoluciones. RMA Nº_____
AlphaSHield Inc. reparará las unidades defectuosas que no estén en programa de garantía con un cargo nominal. Póngase en contacto con el representante de ventas de AlphaShield para obtener más detalles y precios.

Descripción del problema: _____
_____
_____
_____
_____